

Personuppgiftspolicy

1. Tillämplighet och omfattning

Denna Policy är tillämplig på alla anställda medarbetare i Skara stiftsorganisation.

Denna policy ska, på begäran och i enlighet med tillämplig lag, göras tillgänglig för Integritetsskyddsmyndighet-en, vilken är svensk tillsynsmyndighet för behandling av personuppgifter.

I den mån dataskyddsförordningen ((EU) 2016/679) fastställer ytterligare krav ska den tillämpas vid sidan av denna policy. Om någon del av denna policy strider mot dataskyddsförordningen ska dataskyddsförordningen tillämpas i den berörda delens ställe.

2. Syfte

Denna policy har tagits fram i syfte att säkerställa att stiftsorganisationen behandlar personuppgifter på ett lagligt och korrekt sätt med hänsynstagande till individens rätt till skydd av integritet. Policyn förklarar stiftsorganisationens inställning vad gäller skydd av personuppgifter och fastställer instruktioner för hur dessa ska hanteras.

3. Definitioner

Med "personuppgifter" menas i denna policy all information som direkt eller indirekt går att härleda till en identifierbar levande person, särskilt med hänvisning till en identifierare såsom namn, ID-nummer, lokaliseringssuppgifter eller onlineidentifikatorer eller faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Med "registrerad" menas i denna policy en identifierbar levande person vars personuppgifter är föremål för behandling.

4. Policy

Stiftsorganisationen ska följa dataskyddsförordningen och utöva sin verksamhet på ett sätt som respekterar individers integritet. I detta avseende gäller följande för stiftsorganisationens behandling av personuppgifter:

- Laglighet, korrekthet och öppenhet. Insamling, användning och övrig behandling av personuppgifter ska ske på ett lagligt, korrekt och öppet sätt gentemot den registrerade. Stiftsorganisationen ska underlätta för den registrerade att utöva sina rättigheter i enlighet med dataskyddsförordningen.
- Ändamålsbegränsning. Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får senare inte behandlas på ett sätt som går emot dessa ändamål. Stiftsorganisationen ska tillse att det finns rutiner för gallring eller avidentifiering av personuppgifter vars behandling inte längre är nödvändig för sina ursprungliga ändamål.
- Endast behandling på laglig grund. Personuppgifter ska endast behandlas om en laglig grund finns för behandlingen.
- Lagringsminimering. Stiftsorganisationen ska endast lagra personuppgifter så länge detta är nödvändigt för att uppfylla verksamhetens fastställda behov av behandlingen. När lagring inte längre är nödvändig av dessa skäl, ska stiftsorganisationen radera, begränsa eller anonymisera personuppgifterna i fråga.

- Information om behandling av personuppgifter. Stiftsorganisationen ska, i enlighet med dataskydds-förordningen, tillhandahålla information till berörda personer om behandlingen av personuppgifter.

- Åtkomst till personuppgifter. Stiftsorganisationen ska ge åtkomst till personuppgifter i enlighet med dataskyddsförordningen.

- Invändningar mot behandling. Stiftsorganisationen ska tillse att den registrerade kan invända mot be-handling som utförs på basis av ett allmänt eller berättigat intresse eller i direkt marknads-förings-syfte och ska godta en sådan begäran när det är aktuellt.

- Dataportabilitet. Personuppgifter ska, på begäran från den registrerade och under förutsättning att det är tekniskt möjligt, överföras från stiftsorganisationen till en annan organisation. I vilket fall som helst ska stiftsorganisationen, i de fall det är aktuellt enligt dataskyddsförordningen, kunna lämna ut personuppgifter i ett allmänt använt, strukturerat och maskinläsbart format och underlätta så långt möjligt för den registrerade att själv överföra sina uppgifter till en annan organisation.

- Uppgiftsminimering och korrekthet. Personuppgifter ska vara adekvata, relevanta och inte för omfattande för behandlingens ändamål och ska uppdateras vid behov. Felaktiga uppgifter ska rättas eller kompletteras, antingen på stiftsorganisationens eget initiativ eller på den registrerades begäran.

- Anlitande av personuppgiftsbiträden. Stiftsorganisationen får tilldela tredje parter uppgifter vilka innebär att de kommer att ha åtkomst till och behandla personuppgifter på stiftsorganisationens vägnar (personuppgiftsbiträden). Stiftsorganisationen ska alltid säkerställa att personuppgiftsbiträdena uppfyller denna policys krav samt krav som följer av dataskyddsförordningen. Stiftsorganisationen ska sär-skilt ingå biträdesavtal med personuppgiftsbiträden för att kunna ställa krav på hur personuppgifterna får behandlas.

- Personuppgifter utanför EU/EES. Stiftsorganisationen ska följa de restriktioner för överföring av personuppgifter till mottagare utanför EU/EES som ställs upp av dataskyddsförordningen.

Integritet och konfidentialitet. Stiftsorganisationen ska utvärdera risker i relation till sin behandling av personuppgifter samt vidta lämpliga tekniska och organisatoriska åtgärder. Åtgärderna ska säkerställa en tillräcklig nivå av konfidentialitet och säkerhet. Stiftsorganisationen ska i synnerhet säkerställa skydd av personuppgifter mot obehörig eller otillåten behandling, förlust, förstöring eller skada genom olyckshändelse.

- Inbyggd integritet (privacy by design). Stiftsorganisationen ska säkerställa att IT-system och rutiner utformas med dataskyddsförordningens krav i åtanke redan från början.

- Dataskydd som standard (privacy by default). Stiftsorganisationen ska säkerställa att personuppgifter inte behandlas i onödan och att IT-system och rutiner uppfyller dataskyddsförordningens krav som standard. Integritetsskydd ska vara regeln, inte undantaget.

5. Ansvar och överträdelser

Samtliga anställda medarbetare ska ha kännedom om stiftsorganisationens inställning vad gäller skydd av personuppgifter och ska samarbeta med arbetsgivaren för att policyn ska kunna uppfyllas. Leverantörer och andra samarbetspartners förväntas följa denna policy i den mån de behandlar personuppgifter på stiftsorganisation-ens vägnar.

Överträdelser av denna policy kan leda till disciplinära och/eller rättsliga åtgärder. Samtliga anställda medarbetare och samarbetspartners är skyldiga att omedelbart rapportera misstänkta överträdelser av denna policy till närmaste chef eller, för samarbetspartners, till stiftsorganisationen.

Antagen av stiftsstyrelsen 19 april 2018